UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,927	03/19/2004	Steven T. Baker	3961-US	8218

56436 7590 12/10/2008

3COM CORPORATION
350 CAMPUS DRIVE
MARLBOROUGH, MA 01752-3064

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/804,927	BAKER, STEVEN T.	
	Examiner	Art Unit	
	BRANDON S. HOFFMAN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15,19 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15,19 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15, 19, and 20 are pending in this office action.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 17, 2008, has been entered.

3. Applicant's arguments, filed October 17, 2008, have been considered but are not persuasive.

Claim Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

5. Claims 1-15, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berson et al. (U.S. Patent No. 6,123,456) in view of Eichert et al. (U.S. Patent No. 6,393,474).

Regarding claim 1, Berson et al. teaches a method of securing a network interface device installed on a host comprising:

- Initializing the network device without transmit functions (fig. 3, ref. num 306);
- Receiving notification that the host has been authenticated (fig. 3, ref. num 314); and
- In response to receiving notification that the host has been authenticated, enabling transmit functions of the network device (fig. 3, ref. num 318).

Berson et al. does not teach the network interface device is secured, but rather a network device attached to the host device is secured.

Eichert et al. teaches securing the network interface device without transmit functions (col. 7, lines 31-43) and the notification of authentication is received on the host on which the network interface is installed (col. 7, lines 31-43, the policy information is transferred to the smart NIC of the host that the NIC is installed).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine securing the network interface card from transmit

functions, as taught by Eichert et al., with the method of Berson et al. It would have been obvious for such modifications because this securing can be used to control bandwidth congestion issues on a network with the use of a policy (see col. 7, lines 31-43 of Eichert et al.).

Regarding claim 2, Berson et al. as modified by Eichert et al. teaches wherein initializing the network interface device comprises initializing the network interface device without receive functions (see col. 4, lines 60-62 of Berson et al.).

Regarding claim 3, Berson et al. as modified by Eichert et al. teaches further comprising in response to receiving notification that the host has been authenticated, enabling receive functions of the network interface device (see fig. 3, ref. num 318 of Berson et al.).

Regarding claims 4 and 20, Berson et al. as modified by Eichert et al. teaches wherein enabling receive functions of the network interface device comprises routing received data to a network stack (see col. 2, lines 22-24 of Berson et al.).

Regarding claim 5, Berson et al. as modified by Eichert et al. teaches further comprising accessing a firewall policy server to download firewall policy information that is used by a firewall on the network interface device after enabling transmit functions of the network interface device (see fig. 3, ref. num 308 and 310 of Berson et al.).

Regarding claim 6, Berson et al. as modified by Eichert et al. teaches wherein accessing a firewall policy server is performed before transmitting or receiving data from other clients or servers (see fig. 3, ref. num 308 and 310 of Berson et al.).

Regarding claim 7, Berson et al. as modified by Eichert et al. teaches wherein accessing a firewall policy server comprises authenticating the firewall policy server (see col. 1, lines 43-45 of Berson et al.).

Regarding claim 8, Berson et al. as modified by Eichert et al. teaches wherein receiving notification that a host has been authenticated includes receiving notification that the host has been authenticated for a role, and wherein accessing a firewall policy server comprises downloading firewall policy information for the role (see col. 4, lines 60-62 of Berson et al.).

Regarding claim 9, Berson et al. as modified by Eichert et al. teaches further comprising receiving firewall policy information communicated to the host and using the firewall policy information at a hardware based firewall on the network interface device (see fig. 1, ref. num 112 of Berson et al.).

Regarding claim 10, Berson et al. teaches a network interface device for use in a host on a network, the network interface device comprising:

- A network port adapted to send and receive network information (fig. 2, ref. num 234); and
- A module that disables at least one of transmit and receive functionality to the network port of the network device until the network device is notified that the host has been authenticated (fig. 3, ref. num 314 and 318).

Berson et al. does not teach the network interface device is secured, but rather a network device attached to the host device is secured.

Eichert et al. teaches securing the network interface device without transmit functions (col. 7, lines 31-43) and the notification of authentication is received on the host on which the network interface is installed (col. 7, lines 31-43, the policy information is transferred to the smart NIC of the host that the NIC is installed).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine securing the network interface card from transmit functions, as taught by Eichert et al., with the device of Berson et al. It would have been obvious for such modifications because this securing can be used to control bandwidth congestion issues on a network with the use of a policy (see col. 7, lines 31-43 of Eichert et al.).

Regarding claim 11, Berson et al. as modified by Eichert et al. teaches further comprising a firewall that is adapted to prevent the network interface device from communicating with other devices according to firewall policy information stored at the firewall (see fig. 1, ref. num 112 of Berson et al.).

Regarding claim 12, Berson et al. as modified by Eichert et al. teaches further comprising nonvolatile memory, and wherein the firewall policy information is stored in the nonvolatile memory (see fig. 2, ref. num 216 of Berson et al.).

Regarding claim 13, Berson et al. as modified by Eichert et al. teaches wherein the network interface device is adapted to receive firewall policy information from a firewall policy server (see fig. 5 of Berson et al.).

Regarding claim 14, Berson et al. as modified by Eichert et al. teaches wherein the network interface device is embodied as a network interface card (see fig. 2, ref. num 250 of Eichert et al.).

Regarding claim 15, Berson et al. as modified by Eichert et al. teaches wherein the network interface device is embodied as a Secure CardBus network card (see fig. 2, ref. num 250 of Eichert et al.).

Regarding claim 19, Berson et al. teaches a method of securing a network interface device installed on a host comprising:

- Initializing the network device without receive functions (fig. 3, ref. num 306);
- Receiving notification that the host has been authenticated (fig. 3, ref. num 314); and
- In response to receiving notification that the host has been authenticated, enabling receiving functions of the network device (fig. 3, ref. num 318).

Berson et al. does not teach the network interface device is secured, but rather a network device attached to the host device is secured.

Eichert et al. teaches securing the network interface device without transmit functions (col. 7, lines 31-43) and the notification of authentication is received on the host on which the network interface is installed (col. 7, lines 31-43, the policy information is transferred to the smart NIC of the host that the NIC is installed).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine securing the network interface card from transmit functions, as taught by Eichert et al., with the method of Berson et al. It would have been obvious for such modifications because this securing can be used to control bandwidth congestion issues on a network with the use of a policy (see col. 7, lines 31-43 of Eichert et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON S. HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon S Hoffman/
Primary Examiner, Art Unit 2436